Data Privacy Detective Podcast – Episode 68: Catching Cyber-Criminals With Digital Forensics

Jul 08, 2021

Categories:

Blogs
Podcast
Technology Blog

Authors:

Joseph J. Dehner

Ransomware attacks, data breaches, digital theft – on the rise. Who are the cyber-criminals? Can they be traced? And what can a company do to minimize risk and respond to an incident?

Joining us for a tour of the dark side of the digital age is Bill Corbitt, Vice President of Digital Forensics and Incident Response at Intersec Worldwide. www.intersecworldwide.com, a US-based team of former federal cybersecurity experts who have worked on some of the world's largest security breaches. The firm was named a 2021 top Digital Forensics & Incident Response firm by Enterprise Security Magazine. Bill's team has addressed serious incidents for many Fortune 100 companies. In this podcast he shares insights into dealing with ransomware attacks, data theft, and the aftermath.

Ransomware attacks are conducted by sophisticated criminal enterprises, usually operating from data havens where government seldom prosecutes them for attacks abroad. They probe for vulnerabilities and find attack vectors into a company's IT system, freeze digital operations, then post a ransom demand before releasing their grip that can paralyze the victim's business.

Modern digital forensic techniques can generally identify the attackers. The quicker an attacked business engages a forensic expert, the more likely it is that the perpetrator can be identified. Ransomware attackers increasingly have two waves of ransom demand – the first to unlock the system, the second to promise not to release exfiltrated data to the world. Every ransomware attack should be viewed as a data breach, though it is possible for a forensics expert to determine if data has been taken rather than only temporarily encrypted.

The Convention on Cybercrime, aka the Budapest Convention, arose in 2004. By July 2021 there were 66 members and 11 signatories. The Convention promises cross-border cooperation in combating cybercrime. But Russia, China, and India and many countries have

not joined. In these and other countries, cybercrime is not a significant political issue as it deals primarily with foreign attacks.

Cybercrime, like all crime, will not disappear. If there is money to be made, criminals will seek it. Minimizing risk is essential. Businesses should constantly upgrade their entire IT systems, eliminating weak points and discarding outdated elements. Those with access to company computers and systems need training and discipline to view company property and data with care.

Should ransom be paid if a ransomware attack happens? Barring laws against making a payment, businesses will be under obvious pressure to restore their systems, and ransomware insurance is available. And if ransom is not paid, cyber-gangs will threaten to release the data after exfiltrating it through a second ransom demand.

If you have ideas for more interviews or stories, please email info@thedataprivacydetective.com.

FBT Gibbons